



National Aeronautics and
Space Administration

NSTS 37310

Lyndon B. Johnson Space Center
Houston, Texas 77058

SPACE SHUTTLE

**SPACE SHUTTLE PROGRAM
SAFETY RISK RANKING METHODOLOGY**

APRIL 6, 1995

REVISION LOG

REV LTR	CHANGE NO	DESCRIPTION	DATE
		BASELINE ISSUE (Reference: Space Shuttle PRCBD S060333R1, dated 2/17/95).	04/06/95

NSTS 37310 – Space Shuttle
Space Shuttle Program Safety Risk Ranking Methodology

LIST OF EFFECTIVE PAGES

April 6, 1995

The current status of all pages in this document is as shown below:

<u>Page No.</u>	<u>Change No.</u>	<u>PRCBD No.</u>	<u>Date</u>
i – vi	Baseline	S060333R1	February 17, 1995
1-1 – 1-2	Baseline	S060333R1	February 17, 1995
2-1 – 2-2	Baseline	S060333R1	February 17, 1995
3-1 – 3-2	Baseline	S060333R1	February 17, 1995
4-1 – 4-4	Baseline	S060333R1	February 17, 1995
5-1 – 5-2	Baseline	S060333R1	February 17, 1995
6-1 – 6-16	Baseline	S060333R1	February 17, 1995

NSTS 37310

SPACE SHUTTLE

**SPACE SHUTTLE PROGRAM
SAFETY RISK RANKING METHODOLOGY**

THIS PAGE INTENTIONALLY LEFT BLANK

FOREWORD

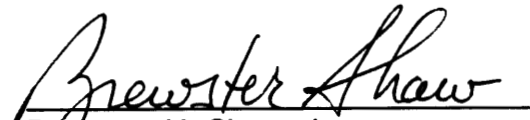
Efficient management of the Space Shuttle Program (SSP) dictates that effective control of program activities be established. Requirements, directives, procedures, interface agreements, and system capabilities shall be documented, baselined, and subsequently controlled by SSP management.

Program requirements controlled by the Director, Space Shuttle Operations, are documented in, attached to, or referenced from Volume I through XVIII of NSTS 07700.

NSTS 37310 details the Risk Ranking Methodology for the SSP and shall provide a method for ranking in relative order of risk SSP candidate projects associated with safety. The content of this document is the responsibility of the SSP Chief Engineer Office and the Safety and Obsolescence (S&O) Board reporting to that office. In the event there is a conflict between the requirements of NSTS 07700 and this document, NSTS 07700 shall take precedence.

All elements of the SSP must adhere to these baselined requirements. When it is considered by the Space Shuttle Program element/project managers to be in the best interest of the SSP to change, waive or deviate from these requirements, an SSP Change Request (CR) shall be submitted to the Program Requirements Control Board (PRCB) Secretary. The CR must include a complete description of the change, waiver or deviation and the rationale to justify its consideration. All such requests will be processed in accordance with NSTS 07700, Volume IV, and dispositioned by the Director, Space Shuttle Operations, on a Space Shuttle PRCB Directive (PRCBD).

Once initially baselined by the Director, Space Shuttle Operations, this document is under the control of the Systems Integration Review (SIR), and changes will not normally require Space Shuttle PRCB approval. However, changes that do not have unanimous agreement regarding technical credence or that have SSP cost/schedule impacts shall be forwarded to the Space Shuttle PRCB for disposition.



Brewster H. Shaw, Jr.
Director, Space Shuttle Operations

THIS PAGE INTENTIONALLY LEFT BLANK

CONTENTS

NSTS 37310

1.0	APPLICATION	1–1
2.0	APPLICABLE DOCUMENTS	2–1
3.0	INTRODUCTION	3–1
3.1	BACKGROUND	3–1
3.2	OBJECTIVE	3–2
3.3	PURPOSE	3–2
3.4	APPROACH	3–2
4.0	RISK RANKING METHODOLOGY	4–1
5.0	RESULTS AND THEIR MEANING	5–1
6.0	DESIGN CRITERIA FOR SAFE SYSTEMS	6–1
6.1	STRUCTURAL REQUIREMENTS	6–1
6.2	ISOLATION	6–2
6.3	INTERLOCKS	6–3
6.4	PARTS AND MATERIALS	6–4
6.5	ENERGY DISSIPATION	6–6
6.6	EXPOSURE WINDOW	6–7
6.7	HUMAN IMPACTS	6–8
6.8	DETECTION	6–9
6.9	MAINTENANCE FACTORS	6–11
6.10	SIGNIFICANT FAILURE HISTORY	6–12

TABLES

NSTS 37310

6.1 EFFECTIVENESS 6–15

1.0 APPLICATION

SSP improvements associated with Safety are to be evaluated by the S&O Board for merit and acceptability for incorporation into the SSP. Arranging the candidates in a relative order of the risk that is to be eliminated or reduced allows the best yield of Safety improvement for resources applied. The Risk Ranking Methodology baselined in this document provides a method to rank the candidate Safety improvements. The Safety, Reliability, and Quality Assurance (SR&QA) organizations supporting the SSP shall apply this methodology to a candidate Safety improvement and report the results to the S&O Board. The Methodology baselined in this document is also included in NSTS 22973, Revision E, Management Safety Assessment for Space Shuttle Program document.

THIS PAGE INTENTIONALLY LEFT BLANK

2.0 APPLICABLE DOCUMENTS

The following documents of the date and issue shown form a part of this document to the extent specified herein. “(Current Issue)” is shown in place of a specific date and issue when the document is under Space Shuttle PRCB control. The current status of documents shown with “(Current Issue)” may be determined from NSTS 08102, Program Document Description and Status Report.

NSTS 07700
(Current Issue)

Program Definition and Requirements

Ref. Foreword

NSTS 07700
Volume IV
(Current Issue)

Configuration Management Requirements

Ref. Foreword

NSTS 22973
Revision E

Management Safety Assessment for Space Shuttle Program

Ref. Para. 1.0, 3.2

THIS PAGE INTENTIONALLY LEFT BLANK

3.0 INTRODUCTION

To successfully rank Shuttle components for safety risk reduction, the following three conditions should exist:

- a. Clear objectives of the prioritization and risk management effort.
- b. An existing source of risk information.
- c. A prioritization methodology that is manageable and conducive to consistent results.

The construction of a ranking scale can be composed of (1) a set of fundamental safety observations, (2) a mathematical transformation from observations to values, and (3) a quantitative result used for comparison and decision making.

We use engineering judgment and the results of analysis and testing to assess a set of safety design criteria relating to a given candidate cause. This assessment is the design and operational controls found in the Shuttle hazard analyses. It is understood that given many successful flights of the Space Shuttle, the hazard controls have worked very well. However, the program continues to operate with “accepted risks”, and given the high energy and dynamic systems, there is always room for safety improvement.

We assess safety risks according to information in the hazard reports that may include Failure Modes and Effects Analysis (FMEA)/Critical Items Lists (CILs) as causes. Some causes are “ground ruled” out of FMEA analysis and must be addressed independently within the hazard reports. For safety analysis, the hazard report relies on design characteristics and operational procedures to justify that it is safe to fly.

3.1 BACKGROUND

The source of risk information (i.e., the information and referenced documents within the hazard reports) for this methodology is qualitative and ranks catastrophic events by prioritization matrices (a 3X4 matrix of likelihood vs. severity). Many comparisons of catastrophic events can be made but are sometimes subjective, emotional, and of different techniques. A complete Probabilistic Risk Assessment (PRA) would be the most desirable analysis, but a PRA is a labor intensive effort requiring many system experts, a complete understanding of PRA analysis, and proper management of that effort.

The following text describes a methodology for comparing candidate causes of catastrophic events. The ranking is based on consistently applied safety design controls and operational procedures that reduce the likelihood a hazardous condition will result in a catastrophic event. Although quantitative results are produced, they are simply numerical representations of a judgmental process.

3.2 OBJECTIVE

The objective of the risk ranking methodology is to rank safety risk issues for the Space Shuttle Program and provide a decision aid for funding risk reduction design or operation. The Space Shuttle Program Management Safety Assessment (MSA) will use this methodology to identify significant safety risks in support of a risk–reduction program. The MSA document (NSTS 22973) is published annually by the SR&QA directorate at the Johnson Space Center (JSC) and identifies selected SSP risks in support of a risk–reduction program. The MSA is performed and documented to focus management attention on selected risks that were chosen from the group of risks that could result in loss of vehicle or crew, and to enhance communication of these risks to all management and technical personnel. This assessment includes Space Shuttle integration, Shuttle elements, launch and landing, government–furnished equipment, contractor–furnished equipment, and Orbiter experiments.

3.3 PURPOSE

The purpose of this methodology is to rank candidate causes that are considered significant enough to warrant action by the SSP and to evaluate the risk reduction achieved by proposed “fixes”.

3.4 APPROACH

The methodology will address a limited list of candidate causes, and will not require reevaluating the Space Shuttle for new hazardous conditions.

4.0 RISK RANKING METHODOLOGY

The procedure begins with a system that contains a credible hazardous cause. The cause can be a hardware failure, an unsafe act, or a combination of unsafe conditions. These will be called candidate causes. Candidate causes can be proposed from any source.

When the system is identified to an appropriate level of detail, a hazardous condition is identified with a single-candidate cause. The cause should have already been identified in the hazard analyses.

The formula used is:

$$RRS = DCp \times [(DCs) (E)]$$

Where: RRS is the RISK RANKING SCORE

DCp – Describes the PRIMARY DESIGN CONTROL of the system. That is, the system is designed to operate with absolutely NO FAILURES and does not include a secondary, emergency, or backup means of getting us out of a hazardous condition. Consider a flawless flight. All systems function as they were designed and no backup, redundancy, or emergency procedure is used to abate a failure.

DCs – Describes the SECONDARY DESIGN CONTROL of the system. That is, the system is designed to abate the effects of a PRIMARY DESIGN CONTROL failure. These could include redundancy or crew actions.

E – EFFECTIVENESS of the SECONDARY DESIGN CONTROL. This describes the condition the vehicle will be in if the SECONDARY DESIGN CONTROL works as designed. This may be a complete hazard isolation, substandard isolation (continue with full mission), substandard isolation (continue with minimum duration mission), safe configuration (next primary landing site), safe configuration (intact abort scenario), or contingency abort emergency landing, or any other condition that will likely result in loss of vehicle and crew.

Effectiveness has no effect on the PRIMARY DESIGN CONTROL (remember, if the PRIMARY DESIGN CONTROL functions as it was designed, then we do not need a SECONDARY DESIGN CONTROL). EFFECTIVENESS can often be found in the operational Flight Rules, or ground operating procedures.

STEP 1 – Identify WHAT the candidate cause is and WHEN it occurs. This step identifies the specific hazard cause, its hazardous condition, and the applicable hazard report. Conditions of interest may include induced and natural environments. There is conceivably no limit to the number of causes that can be

addressed at one time, but it is best to keep that number to a minimum and try not to assess conflicting causes (e.g., valve fails open or closed).

STEP 2 – Identify the PRIMARY DESIGN CONTROLS we use to prevent the candidate cause from occurring by asking the question, “which of the DESIGN CRITERIA FOR SAFETY SYSTEMS (below) is used as a PRIMARY DESIGN CONTROL?” The applicable hazard analysis will reference the required data (CIL, Flight Rules, Launch Commit Criteria [LCC], Operations and Maintenance Requirements and Specifications [OMRS], etc.) needed for the analysis, other data not specifically identified in the hazard report (e.g., Program Compliance Assurance and Status System [PCASS], Problem Reporting and Corrective Action [PRACA], certification data, etc.) can also be used. Remember, do not include backups, redundancy, or emergency procedures. Use a set of guidelines to assess the control. Rate the design or procedure on a scale of 0 to 5, (0 for a weak controls and 5 for a strong controls). If a DESIGN CRITERIA does NOT apply and cannot be used as a design control, mark it with an N/A (Not Applicable).

NOTE: Justification for the rating (0 – 5) and why a design criteria is considered not applicable must be documented and provided with the candidate safety issue submittal and/or as part of the management safety assessment. Without the justification, the candidate safety issues and the Management Safety Assessment results cannot be evaluated by management.

STEP 3 – Sum the ratings (the values of 0 – 5) for each design confidence factor (ignore the N/A's). The maximum rating sum will be 50, minimum 0.

$$ACF = \sum_{i=1}^{i=n} R_i$$

ACF – Aggregate Confidence Factor

n – Number of design controls

R_i – Confidence Factor for the ith criterion

STEP 4 – Multiply the number of design confidence factors used in the rating by 5 (ignore the N/A's). The maximum DC product will be 50, minimum 0. This value will always be equal to or greater than the value found in STEP 3.

$$NF = (5 \times n)$$

NF – Normalizing Factor

STEP 5 – Subtract the value found in STEP 3 from the value in STEP 4.

$$NF - ACF = (5 \times n) - \left[\sum_{i=1}^{i=n} Ri \right]$$

STEP 6 – Divide the value found in STEP 5 by the value found in STEP 4. Set DCp equal to this quotient.

$$DCp \text{ or } DCs = \frac{NF - ACF}{NF} = \frac{(5 \times n) - \left[\sum_{i=1}^{i=n} Ri \right]}{(5 \times n)}$$

$$DCp \text{ or } DCs = 1 - \left[\frac{\sum_{i=1}^{i=n} Ri}{(5 \times n)} \right]$$

STEP 7 – Identify the SECONDARY DESIGN CONTROL (if any) used to minimize the hazardous effects of the candidate cause, should the PRIMARY DESIGN CONTROL fail to perform resulting in a hazardous condition. This can include anything from identical redundancy to a contingency operation that buys time until something else can be done. If there are no SECONDARY DESIGN CONTROLS, DCs and E will both be set equal to 1.0.

Perform the same analysis with the same DESIGN CRITERIA FOR SAFE SYSTEMS as in STEP 2 for the SECONDARY DESIGN CONTROL system. Repeat STEPS 3 – 6 for the SECONDARY DESIGN CONTROL system.

STEP 8 – Set DCs equal to the quotient of STEP 6 for the SECONDARY DESIGN CONTROL system.

STEP 9 – Identify the EFFECTIVENESS of the SECONDARY DESIGN CONTROL. Assuming the SECONDARY DESIGN CONTROL functions as designed (despite the results of STEP 6) identify from the EFFECTIVENESS table (see Table 6.1) in what situation the vehicle will be.

STEP 10 – Set the value of “E” as the number in parenthesis located in the appropriate EFFECTIVENESS.

STEP 12 – Calculate the RISK RANKING SCORE (RRS) per the following formula:

$$RRS = DCp \times [(DCs)(E)]$$

THIS PAGE INTENTIONALLY LEFT BLANK

5.0 RESULTS AND THEIR MEANING

When several candidate causes have been assessed, they may be listed according to their RRS value. In this analysis, 1.000 is the maximum score (worst situation) and 0.000 is the minimum score (best situation). The highest scores can be investigated to identify where risks may be reduced.

THIS PAGE INTENTIONALLY LEFT BLANK

6.0 DESIGN CRITERIA FOR SAFE SYSTEMS

6.1 STRUCTURAL REQUIREMENTS

The system is analyzed and/or tested for adequate structural requirements (e.g., factors of safety, margins of safety, strength, fatigue life determination, fracture critical requirements, or hardness values for load bearing material).

For DCp: How well can the structural properties of the primary system preclude the development of the candidate cause?

For DCs: How well can the structural properties of the secondary design control system preclude the failure of the secondary design control?

Consider the following in assessing this design confidence factor:

- a. Structural design for margin of safety, factor of safety, yield, ultimate, proof, burst.
- b. Structural design for fracture critical requirements.
- c. Nondestructive Examination (NDE) for indications of material degradation in the form of cracks, flaws, voids, inclusions, and defects (magnetic particle, dye penetrant, X-ray, eddy current, ultrasonic, etc.).
- d. Fatigue life testing.
- e. Visual inspections.
- f. Dimension measurements.
- g. Certification by analysis and/or testing or by similarity.
- h. Hardness testing.
- i. Shock, vibration, and acoustic testing.
- j. Preload applications.
- k. Design for tensile stress, yield strength, elongation, reduction.
- l. Design for bending allowances.
- m. Design for brittleness.
- n. Torque applications.

- o. Terminal strength.
- p. Qualification test levels – The system has been qualified at test levels well above planned mission requirements.

Scoring Examples: 0 – Presently operating at a factor of safety less than required (even if it is by waiver), no NDE during certification, no proof testing, no hardness checks, no terminal pull tests, no torques tests, no visual checks, no certification tests.

- 5 – Designed and certified with high margins of safety, tested for fatigue life determination, hardness measurements, tested fracture critical components, hardness tested, properly torqued with calibrated wrench, terminal pull tested.

6.2 ISOLATION

The system is designed to employ isolation measures to preclude damage due to induced or natural environments, or a primary design control failure (e.g., distance, barriers, filters, purge systems, deflection, containment, or continuous lines without breaks).

For DCp: How well is the primary system isolated from the candidate cause?

For DCs: How well is the secondary design control system isolated from a failure cause?

Consider the following in assessing this design confidence factor:

- a. Located away from common cause failures
- b. Guarded with barriers, (pressure, mechanical, thermal, electrical)
- c. Purges that remove toxic gases
- d. Protected from exposure to hostile environment (moisture, fungus, salt fog, air, etc.)
- e. Designed to limit “breaks” in lines in the form of flanges, welds, electrical terminals, connections
- f. Isolated from other equipment resulting in minimal damage if it disintegrates
- g. Designed to limit success paths routed through the same path
- h. Designed to limit leak paths

- i. Designed with double-walled containment
- j. Insulation resistance

Scoring Examples:

- 0 – System designed with numerous flanges, no purges, no flywheel barriers, installed close to other susceptible equipment, leaving component exposed to weather with no protection, no thermal protection, exposed wiring, exposed hot surfaces.
- 5 – System designed with double-walled containment, continuous lines with little or no residual stress, system purges, strong housing or guards to deflect shrapnel, filters that can block contamination, sealed protection from elements and environment, Thermal Protection System (TPS), electrical insulation.

6.3 INTERLOCKS

The system is precluded from operating in an unsafe condition by employing an interlock (e.g., safety wiring, switch locks, interlocks that must be operated in a specific sequence (e.g., Ground Launch Sequencer [GLS], Redundant Set Launch Sequence [RSLS]), ignition sequences).

For DCp: How well can interlocks in the primary system preclude the development of the candidate cause?

For DCs: How well can interlocks in the secondary design control system preclude a failure of the secondary design control?

Consider the following in assessing this design confidence factor:

- a. Designed to use ignition trains
- b. Designed with safety switches
- c. Designed with fuses or circuit breakers
- d. Employs Ground Launch Sequencer, Redundant Set Launch Sequencer
- e. Designed with switch guards
- f. Mechanical systems designed with detents
- g. Designed to use specific starting procedures
- h. Controlled with the use of computer software

- i. Employs lockwire
- j. Confirmation prior to implementation
- k. Circuit not active until you need it
- l. Employs the use of inhibits

Scoring Examples: 0 – Hardwire connections directly to high energy component without a safety switch, no safety wiring, no switch guards or covers, no fuse or circuit breaker protection, continuously armed system.

5 – Ground Launch Sequencer, ignition trains, lockwire, switch guards and covers, fuses, circuit breakers, software sequencing, system off until required, mechanical detent in booster safe and arm device.

6.4 PARTS AND MATERIALS

PARTS AND MATERIALS (MECHANICAL) – The system is designed with material or material types such that no mechanical part can adversely damage itself or another material (e.g., cracking, gouging, fretting, friction, effects of contamination, extreme heat, cryogenics).

PARTS AND MATERIALS (CHEMICAL) – The system is designed with material or material types such that no part can chemically damage itself or another material (e.g., corrosion, incompatible materials, combustion, exothermic or endothermic reactions).

PARTS AND MATERIALS (ELECTRICAL) – The system is designed with material or material types such that no part can electrically adversely damage itself or another material (e.g., short circuit, expanding or collapsing field, arcing, electromagnetic radiation).

For DCp: How well can the material properties of the primary system preclude the development of the candidate cause?

For DCs: How well can the material properties of the secondary design control system preclude a failure of the secondary design control?

Consider the following in assessing this design confidence factor:

- a. Designed with compatible materials
- b. No susceptibility to radiation damage (alpha, beta, gamma, neutron, ultraviolet, etc.)

- c. Designed to limit material degradation due to use (gouging, fretting, galling, scoring, nicks, scratches, cavitation, arcing, bluing, friction)
- d. Designed to limit flammable materials
- e. Designed to limit corrosive materials
- f. Designed for low voltage where possible
- g. Designed to operate in low oxygen content
- h. Employ the use of compatible lubricants
- i. No susceptibility to magnetic fields
- j. Designed to limit stress corrosion
- k. Designed with heat treatments
- l. Designed for proper resistance
- m. No susceptibility to contamination
- n. Designed to limit possibility of seizure
- o. No susceptibility to pH, acid or base conditions
- p. Test for purity
- q. No susceptibility to thermal or fluid soaking
- r. Designed to preclude short circuits
- s. Designed to not be susceptible to energy sources (ignition sources)
- t. Designed to preclude precipitating particles
- u. Designed to avoid close or tight tolerances
- v. Designed to preclude the generation of debris
- w. Designed to limit corrosion
- x. Designed to avoid ice formation
- y. Designed to preclude inductance
- z. Designed to resist momentary overload
- aa. Designed for solderability
- bb. Designed for long shelf life

- cc. Designed for consistent critical processes for consistent material properties
- dd. Qualification test levels – The system has been qualified at test levels well above planned mission requirements.

Scoring Examples:

- 0 – Excessive fretting due to processing, friction damage, incompatible materials, corrosive environment, fire hazard, high oxygen exposure, radioactive environment, high voltage, use of very flammable or toxic substances, deviating critical processes resulting in different material properties
- 5 – Nonflammable materials, corrosion resistance, use of compatible lubricants, no radiation field, heat resistance, very low voltage, large sealing surfaces, no magnetic fields, material consistency in manufacturing, operates at ambient temperature, parts protection, easy to inspect, no tight tolerances, not susceptible to contamination, no damage from short circuits, etc.

6.5 ENERGY DISSIPATION

The system is designed such that unwanted energy is dissipated by diverting it away (e.g., using grounding straps, relief valves, dumping procedures, sacrificial anodes, shock absorbers, aerodynamics).

For DCp: How well can energy be dissipated in the primary system to preclude the development of the candidate cause?

For DCs: How well can energy be dissipated in the secondary design control system to preclude a failure of the secondary design control?

Consider the following in assessing this design confidence factor:

- a. Designed with relief systems for pressure vessels
- b. Designed with grounding straps
- c. Designed with heat sinks
- d. Designed with lightning protection
- e. Designed with sacrificial anodes (galvanic corrosion)
- f. Use of aerodynamic procedures (e.g., roll reversals upon entry)

- g. Use of pressure vessel dumping procedures
- h. Use of throttling procedures (e.g., “bucket”, 3g throttling)
- i. Designed with shock absorbers
- j. Designed with damping mechanisms
- k. Designed to use braking mechanisms and procedures
- l. Designed to dampen thrust oscillations
- m. Qualification test levels – The system has been qualified at test levels well above planned mission requirements

Scoring Examples: 0 – Pressure vessel with no relief system, no grounding methods, no heat dumping methods for soakback, no pressure dumping procedures, inadequate heat removal, no dampers, no shock absorbers, insufficient braking mechanism, no pyro system shock absorber

 5 – Orbiter TPS, lightning protection, aerodynamic procedures (roll reversals), sacrificial anodes (galvanic corrosion), dumping of propellants, addition of drag chute, no pyro system shock absorber

6.6 EXPOSURE WINDOW

The system is designed to lessen the time a system is susceptible to the hazardous condition (e.g., limiting time hardware is suspended with a crane, limiting time of operation of high energy system, clearing External Tank [ET] prior to ET door closure).

For DCp: What percentage of time is the primary system susceptible to the effects of the candidate cause compared to the total time the primary system is operating?

For DCs: What percentage of time is the secondary design control system susceptible to a failure during the total time the secondary design control is required to abate the effects of a primary design control failure?

Measure exposure per the following:

$$\frac{T_s}{T_o} \times 100 = \% \text{ of time of exposure}$$

Where: Ts = Time of susceptibility to hazardous condition

To = Time of system operation where cause could occur (but not necessarily manifest itself)

Ranking

100% = 0

80 = 1

60 = 2

40 = 3

20 = 4

0 = 5

NOTE: Round value to nearest percent in above chart and use the applicable value

Scoring Examples: 0 – Hazardous condition could be present throughout the operation of the system.

5 – Hazardous condition could be present during less than 1 percent of the system operation.

6.7 HUMAN IMPACTS

The system is designed such that no pathological or human interaction effects can injure personnel (e.g., toxic material, odors, eye irritants, asphyxiation, skin irritants, lung irritants, extreme heat and/or pressure acceleration, disorientation, sharp edges, hot surfaces).

For DCp: How well can the primary design control preclude injury to crew or personnel due to the candidate cause?

For DCs: How well can the secondary design control system preclude injury to the crew or personnel due to the implementation of the secondary design control?

Consider the following in assessing this design confidence factor:

- a. Designed to limit space sickness
- b. Designed to limit disorientation
- c. Designed to preclude sharp edges
- d. Designed to prevent smoke, toxic gases, asphyxiation

- e. Designed to prevent broken glass
- f. Designed to limit mercury in crew cabin
- g. Designed to limit radiation
- h. Designed to preclude poor housekeeping
- i. Designed to preclude hazardous payload chemicals
- j. Designed to prevent loss of cabin pressure
- k. Designed to limit acceleration
- l. Designed to preclude Extravehicular Activity (EVA) operations
- m. Designed to limit particulates in atmosphere
- n. Designed to prevent electrocution
- o. Designed to limit hot/cold surfaces
- p. Designed to limit noise

Scoring Examples: 0 – Mercury exists in the crew cabin, hazardous payload chemicals, EVA operations, broken glass, bird strike penetrates window, space sickness, poor housekeeping

 5 – Supplemental oxygen, first aid available, 3g limitation, carbon filters, air filters, protected sharp edges, electrical insulation

6.8 DETECTION

The system is designed to provide monitoring for hazardous condition symptoms (e.g., detection during flight, caution and warning devices, turnaround testing).

For DCp: How well can the candidate cause be detected before it can result in a catastrophic effect?

For DCs: How well can a secondary design control fault be detected before it may be used to abate a primary system failure?

Consider the following in assessing this design confidence factor:

- a. Employ hydroproof testing
- b. Employ full scale operational testing (e.g., “green run”)

- c. Employ dielectric withstanding voltage testing
- d. Employ launch commit criteria
- e. Employ continuous monitoring (temperature, pressure, voltage, current, levels, etc.)
- f. Employ visual inspection
- g. Employ on-board monitoring capability
- h. Employ pull tests
- i. Employ electrical bond resistance tests
- j. Employ hysteresis testing
- k. Employ test for “noise”
- l. Employ vibration response testing
- m. Employ repeatability testing
- n. Employ output voltage testing
- o. Employ output impedance testing
- p. Employ resistance testing
- q. Employ calibrations testing
- r. Employ bias values testing
- s. Employ cleaning and cleanliness testing
- t. Employ complete Acceptance Test Procedure (ATP) testing
- u. Employ decay testing
- v. Employ hotfire testing
- w. Employ test equipment testing
- x. Employ software/Shuttle Avionics Integration Laboratory (SAIL) testing
- y. Employ timing detection
- z. Employ post mission tests and inspections

- Scoring Examples:
- 0 – No testing during turnaround, no on-orbit testing, no launch commit criteria, no caution and warning, no record of configuration, no hazardous gas detection, no current detection
 - 5 – Full scale test performed each turnaround, NDE performed each processing flow, proof pressure tests each turnaround, continuous monitoring, launch commit criteria, alarms, bells, whistles, lights, field mills

6.9 MAINTENANCE FACTORS

The system is designed to minimize the frequency of remove and replacement and preclude deterioration due to extended use and/or refurbishment (frequent change outs, Remove and Replace [R&R], involved critical processes).

For DCp: How well can the primary system sustain its operating capability with a minimum amount of maintenance or critical processes?

For DCs: How well can the secondary design control system sustain its operating capability with a minimum amount of maintenance or critical processes?

Consider the following in assessing this design confidence factor:

- a. Designed for limited number of maintenance cycles
- b. Designed for long life limits
- c. Designed for long mean time between failures driving R&R
- d. Designed for use of throwaway components
- e. Designed for many power cycles
- f. Designed for many fatigue cycles
- g. Designed for many thermal cycles
- h. Designed to limit the number of critical processes
- i. Designed to minimize the complexity of turnaround processing
- j. Designed for ease of autoclave, hydroclave, casting, curing
- k. Designed for ease of lubrication
- l. Designed for effective flushing when required

- m. Designed for shipping, storing, and handling parts protection
- n. Designed for ease of inspection
- o. Designed to tolerate rough handling
- p. Manufacturing consistency in the mixing of compounds
- q. Designed for easy assembly and installation
- r. Employ limited life requirements
- s. Employ mission life requirements

Scoring Examples: 0 – System must be removed and replaced after each operation for a normal processing flow, system requires tedious critical process, system requires extensive measures to control contamination, system must experience frequent intrusive measurements.

5 – System is not expected to need replacement throughout the life of the program, system is tolerant of rough handling, system is self-sustaining, system does not require careful shipping and storage procedures, system is easy to inspect.

6.10 SIGNIFICANT FAILURE HISTORY

The system is designed such that field and flight failures are not likely (engineering judgment based on failure history in field or flight or critical processes). “SIGNIFICANT” pertains to failures that are directly related to the failure that could result in a catastrophic event if seen during system operation. This does not include test rig failures.

For DCp: How well has the primary system performed in field or flight history in terms of Failure Probability (FP)?

For DCs: How well has the secondary design control system performed in field and flight history in terms of failure probability?

Use the following formula to determine FP:

$$FP = F/NTQ$$

Where: F = Number of failures (from failure data base)
N = Number of flows/flights
T = Number of equivalent tests/operations per flight component
(i.e., how many times is the test/operation performed each flow/flight)
Q = Quantity of components undergoing tests each flow/flight

SIGNIFICANT FAILURE HISTORY Scoring:

- 0 = Frequent – failure ratio – > 0.2
- 1 = Reasonably probable – failure ratio – > 0.10 but < 0.2
- 2 = Possible – failure ratio – > 0.01 but < 0.10
- 3 = Remote – failure ratio – > 0.001 but < 0.01
- 4 = Extremely unlikely – failure ratio – > 0.0001 but < 0.001
- 5 = No failures in the program – failure ratio – < 0.0001

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE 6.1
EFFECTIVENESS

1. (0.167) COMPLETE HAZARD ISOLATION – THE HAZARDOUS CONDITION IS COMPLETELY REMOVED WITH NORMAL REDUNDANCY AS IF THE HAZARDOUS CONDITION HAD NOT OCCURRED.
(EXAMPLE: TROUBLESHOOTING AND CORRECTIVE ACTION TO BRING FAILED SYSTEM BACK ON-LINE).
2. (0.334) SUBSTANDARD ISOLATION, CONTINUE WITH FULL MISSION – THE HAZARD IS ISOLATED, BUT THERE IS LOSS OF REDUNDANCY (EXAMPLE: RCS THRUSTER FAILURE AT ET SEPARATION, REDUNDANCY MANAGEMENT DESELECTS THRUSTER AND ANOTHER THRUSTER IS SELECTED).
3. (0.500) SUBSTANDARD ISOLATION, CONTINUE WITH MINIMUM DURATION MISSION. (EXAMPLE: UNRECOVERABLE LOSS OF ONE APU).
4. (0.667) SAFE CONFIGURATION, NEXT PRIMARY LANDING SITE (KSC, EDWARDS, NORTHRUP) (EXAMPLE: UNRECOVERABLE LOSS OF TWO FUEL CELLS).
5. (0.835) SAFE CONFIGURATION, INTACT ABORT SCENARIO (EXAMPLE: LOSS OF ONE SSME DURING ASCENT PHASE).
6. (1.000) CONTINGENCY ABORT (DITCH) OR LOSS OF VEHICLE CONTROL RESULTING IN POSSIBLE LOSS OF CREW AND VEHICLE DURING ANY PHASE OF THE MISSION OR FLOW. (EXAMPLES: LOSS OF TWO SSME'S DURING EARLY ASCENT OR LOSS OF VEHICLE CONTROL).

THIS PAGE INTENTIONALLY LEFT BLANK